The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
12/8/2009

SUBJECT:
Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (MS09-071)

OVERVIEW:
Two vulnerabilities have been discovered in Microsoft Internet Authentication Service (IAS) server. IAS is the Microsoft implementation of a Remote Authentication Dial-in User Service which performs authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN). Successful exploitation could result in an attacker gaining administrator privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed attacks may cause denial-of-service conditions.

SYSTEMS AFFECTED:

- Windows Server 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows 2008 (R2 Not Affected)

RISK:

Government:
- Large and medium government entities: High
- Small government entities: High

Businesses:
- Large and medium business entities: High
- Small business entities: High

Home users: N/A

DESCRIPTION:
Two vulnerabilities have been discovered in Microsoft Internet Authentication Service (IAS) server. IAS is the Microsoft implementation of Remote Authentication Dial-in User Service (RADIUS). Servers using Protected Extensible Authentication Protocol (PEAP) with Microsoft Challenge Handshake Authentication Protocol v2 (MS-CHAP v2) authentication are affected. PEAP is used to create an encrypted channel between an authentication client, such as a wireless computer, and a PEAP

authenticator, such as an IAS server. MS-CHAP v2 is the authentication protocol used within the encrypted channel provided by PEAP.

Internet Authentication Service Memory Corruption Vulnerability
This vulnerability is caused by the IAS server failing to properly validate PEAP authentication requests. In order to exploit this vulnerability, an attacker would need to create a specially crafted PEAP authentication request. Successful exploitation could result in the attacker gaining administrator privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed attacks may cause denial-of-service conditions.

MS-CHAP Authentication Bypass Vulnerability
This vulnerability is caused by the IAS server failing to properly validate MS-CHAP v2 authentication requests. In order to exploit these vulnerabilities, an attacker would need to create a specially crafted MS-CHAP v2 authentication request. Successful exploitation could result in the attacker gaining elevated privileges. Failed attacks may cause denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Block un-trusted incoming traffic from the Internet at your network perimeter.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS09-071.mspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2505
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3677

Security Focus:
http://www.securityfocus.com/bid/37197
http://www.securityfocus.com/bid/37198